IMPILO Platform - An Innovative Blockchain-Based Global Open Healthcare Social Network

**Thelma Androutsou¹, Michael Kontoulis¹, Konstantinos Bromis^{1*}, Panagiotis Kapsalis¹,
Ioannis Kouris¹, Haralampos Karanikas^{2,3}, Alexandros Christodoulakis³,
Panagiotis Dimitrakopoulos³, Dimitris Askounis¹, Dimitrios Koutsouris³**

¹School of Electrical and Computer Engineering, National Technical University of Athens, Athens, 15773, Greece

²Department of Computer Science and Biomedical Informatics, University of Thessaly, Lamia, 35100, Greece

³Datamed SA, Athens, 15124, Greece

Received July 26, 2021; Revised September 16, 2021; Accepted October 17, 2021

Cite This Paper in the following Citation Styles

(a): [1] Thelma Androutsou, Michael Kontoulis, Konstantinos Bromis, Panagiotis Kapsalis, Ioannis Kouris, Haralampos Karanikas, Alexandros Christodoulakis, Panagiotis Dimitrakopoulos, Dimitris Askounis, Dimitrios Koutsouris, "IMPILO Platform - An Innovative Blockchain-Based Global Open Healthcare Social Network" *Computer Science and Information Technology*, Vol. 9, No. 3, pp. 33 - 49, 2021. DOI: 10.13189/csit.2021.090301.

(b): Thelma Androutsou, Michael Kontoulis, Konstantinos Bromis, Panagiotis Kapsalis, Ioannis Kouris, Haralampos Karanikas, Alexandros Christodoulakis, Panagiotis Dimitrakopoulos, Dimitris Askounis, Dimitrios Koutsouris (2021). *IMPILO Platform - An Innovative Blockchain-Based Global Open Healthcare Social Network*. *Computer Science and Information Technology*, 9(3), 33 - 49. DOI: 10.13189/csit.2021.090301.

Copyright©2021 by authors, all rights reserved. Authors agree that this article remains permanently open access under the terms of the Creative Commons Attribution License 4.0 International License

Abstract The current research project focuses on the development of an innovative social health network and electronic health record system (IMPILO platform) which is based on Blockchain technology. The purpose of this project is to provide a series of health services (e.g. booking of medical appointments and tele-counselling meetings) to both citizens and doctors that would offer a more direct communication and cooperation between them and thus help reduce critical delays in medical care provision. As IMPILO manages health data, in addition to the group of friends found in some forms on all social networks, two additional certain types of user relationships have been defined: Circle of Trust (which includes a limited number of people with full rights to review and modify each user's profile and health record) and Care Team (which consists of the users-doctors that have access to their profile and medical data and can perform certain actions on their behalf). This feature is useful for keeping profiles of elderly and minors. The utilization of the capabilities of the blockchain technology in areas beyond cryptocurrencies is of particular value, especially in the field of health, where the IMPILO platform creates more reliable and durable networks, using the blockchain technology, while helping to the seamless communication between the various stakeholders (doctors, patients,

hospitals, etc.). The decentralized data storage and full control of a patient's consent management process helps overcome issues such as the secure management of sensitive personal data and authorization to access medical data. Thus, blockchain is one of the most important components of the IMPILO platform that acts as a basis for recording all meaningful events in the application and provides security to users for the integrity of their data. The application is accessible via a smartphone application (for both Android and iOS operating systems) and a web interface, with a special emphasis on the design of functional, efficient and easy-to-use user interfaces, taking into account the requirements of the end users of the application and the specifics of the health sector.

Keywords Blockchain Technology, Social Network, Mobile Application, Web Application, Medical Records, Social Health Network, mHealth

1. Introduction

The innovative Blockchain technology promises to

change the way electronic transactions are made across multiple sectors, including healthcare where existing technologies for storing and exchanging medical data and records face several limitations. Issues such as the secure management of sensitive personal data and authorization to access medical data as well as the effective communication between physicians and patients for the provision of personalized treatment can now be addressed through a mechanism that ensures transparency in user authentication and traceability in reading and recording data in a secure, decentralized and distributed manner. At the same time, patients are provided with full control over access, confidentiality and privacy of their data.

The limited efforts until today in the field of healthcare focus on leveraging Blockchain technology as a means of managing public and private keys for providing and withdrawing patient consent in order to provide access to sensitive medical data. The research project described in this document aims to evolve existing approaches by developing an innovative social network of health services and electronic health record system based on Blockchain technology. Through the IMPILO platform, a series of health services are provided to both citizens and doctors, ensuring more direct communication between them and reducing critical delays in medical care provision. The users of the system can have their personal information and medical data securely stored and, upon their consent, physicians can access their medical history, provide follow-up services, and monitor compliance with medication and therapy plans.

Moreover, this implementation aims to develop a social health network that will offer innovative services to patients and doctors, by developing a mobile and web application based on the concept of social networking applications, based on ease of use and optimal user experience. Among other things, the user will be able to communicate with other users, book medical appointments and tele-counselling meetings and have access to electronic health record data integrated from third parties.

The remainder of the article is organized as follows: In section 2, a review of similar projects that use the Blockchain technology in healthcare is presented. Then, in section 3, the main functionalities and interfaces of the platform are described while in section 4 the system architecture of the proposed system is outlined. The evaluation process that was followed is analysed in section 5. Finally, conclusions and future steps are discussed in section 6.

2. Analysis of Existing Healthcare Blockchain Related Projects

Many sectors have traditionally operated without any sort of digitisation but recent technological advancements

and increased needs have even led traditionally paper-based industries to adapt digitisation. The healthcare sector has also undergone significant change, due to increased needs, but adoption hasn't been without hiccups.

To address these needs, many research projects and commercial applications are trying to apply the blockchain technology in various manners in the healthcare sector. In this section we will go over various projects and categorise them based on their main purpose, to explore how blockchain is utilised by them.

2.1. Healthcare Data Infrastructure

These projects' product is the blockchain itself and their aim is first and foremost to supplement the workflow of their potential clients, other organisations. These projects either take advantage of the data integrity validation that blockchain offers or simply uses blockchain in conjunction with a cryptocurrency. Any healthcare organisation could potentially use these solutions since most of these are application agnostic and are not targeted to the healthcare sector specifically.

Notable exceptions, such as Hashed Health exist, which is aimed specifically to healthcare applications and provides additional applications for the handling of data. At some point, Google's deepmind[1] seemed to also use blockchain technology as an auditing mechanism in the handling of healthcare data but the current state of the project and whether it is still active is unclear since no new information has been released for some time.

A common factor that appears in quite a few of these applications is that many opt to not use the decentralised capabilities that blockchain offers. Since the data are usually already controlled by specific organisations which need to conform to specific legal and ethical guidelines at most these blockchains need to be consortium-based ones where many verified organisations have access to them.

The Horizon 2020 research project Curex [2], aims to enhance and secure the information sharing process between healthcare organisations among other things.

2.2. Personal Healthcare Record Management

One step further we can see projects where the focus and the "main product" are the data itself. These are mostly targeted towards the end user themselves and many aim to give control of the medical data to the users themselves instead of the various institutions.

Projects like IRYO [3] have implementations based on openEHR, in an effort to ensure compatibility with as many already existing systems as possible. This project in particular doesn't aim to replace existing infrastructure, but offers users an additional centralised way of managing their data. Data can be stored redundantly in IRYOs servers, the users' devices and the original healthcare

organisation where data already exist. This process is supplemented by the use of cryptocurrency, which is used as payment for the acquisition of their data. A similar project that has essentially the same features is Medrec[4].

2.3. Healthcare Analytics

While projects in the previous sections also contributed to the use of data in medical research, this wasn't the main purpose of these projects. Projects like Doc.ai operate as a data marketplace whose main purpose is to gather medical data from users, so they can be used in research and don't really serve as a general data repository of the users. Doc.ai in particular, uses incorporated systems to anonymise user information and help them find relevant research. It also offers tools specifically to help researchers themselves and help them setup clinical studies easier.

This data marketplace approach is also used by Horizon 2020 research project MyHealthMyData [5], which aims to create an open biomedical information network where patients or hospitals can share anonymised data for research. Blockchain is used in the management and authorisation of data exchanges, to provide traceability and GDPR compliance and automate data sanitisation, through the smart contracts technology embedded in the blockchain.

Another similar research project is the FeatureCloud [6] H2020 project, which instead focuses on client-side data analytics and the sharing of only necessary metadata.

On the other hand, the Panacea [7] H2020 project, which focused on healthcare cybersecurity concluded research on whether the inclusion of blockchain in the project would be beneficial. Reference [8], despite listing some advantages, it ultimately rejected the blockchain inclusion citing GDPR issues and off-chain storage causing more issues that it is solving.

2.4. Medical Devices and IoT Security

Medical devices and especially IoT devices are a new addition to the healthcare ecosystem and a common vector of attack, making their security a priority. In the Spiritus project, Blockchains' role is to serve as a record for the chain of custody and location services of the medical devices, used in conjunction with the already existing RFID/RTLS systems. On the other hand, Neuromesh [9] takes this process a step further. In this project any command executed in the system will be saved in the blockchain allowing anyone with access to it, to inspect exactly what and when each command runs. The pseudo anonymisation characteristics of the blockchain have been proven useful in this case, since they can be used to identify who executed a malicious command. Neuromesh doesn't use a blockchain to store custom codified data but instead uses bitcoin transfers between wallets and its

metadata to transfer information.

2.5. Identity

Proving your identity and Know Your Customer (KYC) processes are very common in the healthcare sector. Blockchain can help by mapping users' physical identities to their digital ones. Accenture's blockchain solution helps patients to handle and share their healthcare records and proof of insurance seamlessly and allows the streamlining of the KYC process.

Travel and healthcare have also been a common issue that have caused issues in patients. The Known Traveler Identity Initiative [10] aims to create a virtual identity for travellers and will use the blockchain in lieu of a certification authority and will be used by participating organisations to issue identifiers which can then be verified by other organisations without relying on a centralised certification authority.

2.6. Supply Chain

Healthcare organisations have significantly complex supply chains that can be difficult to be managed. The Medilegger [11] project aims to smooth the communications between businesses through the use of their blockchain solution. This is achieved through the business rule enforcement where organisations can set up rules that are automatically checked when an action is taken. In addition, it offers product verification, ensuring not only that the product has been delivered to the correct place but also that under legal oversight it can be successfully verified.

Blockpharma [12] on the other hand, takes this concept and applies not to the businesses but to the final consumers themselves. It aims to detect fake medicine through the use of machine learning techniques and ensure the safety of data by using a blockchain to register the medicine and ensure its authenticity.

2.7. Digital Medicine and Care Delivery

A new possibility facilitated by technological advancements is that of digital medicine and care delivery. Instead of using devices to simply store user information, projects which focus on this sector aim to play a more central role in the treatment of patients. Bowhead Health [13] for example, tracks users' daily activities and drug prescription and dosage helping them form habits through gamification and also through a crypto currency that is awarded for keeping up habits. This crypto currency is significantly easier to use since it can be used to buy selected products through the app itself but it can also be used for trading as any other cryptocurrency. In addition, there is the possibility of third-party users taking over hosting of the backend of the application in exchange for

Figure 2. The Social Tab of IMPILO app

3.1. Social Networking

The IMPILO app is a healthcare social network application that contains many features which enable the communication and cooperation between patients and doctors.

During registration, users create a profile that contains personal information, the non-medical and sensitive of which are public to the other users. Doctors also create a clinic profile providing useful information to their patients about clinic location, costs, medical services etc. As IMPILO manages health data, certain types of user relationships have been defined, which also limit access rights to profiles and personal information. In addition to the group of friends found in some form on all social networks, two additional user groups are defined: Circle of Trust and Care Team. Circle of Trust includes a limited

number of people with full rights to review and modify each user's profile and health record (Figure 2). This feature is especially useful for keeping profiles of the elderly and minors. The Care Team group of a user consists of the users-doctors that have access to their profile and medical data and can perform certain actions on their behalf.

The interface of the timeline is one of the main components of the app (Figure 3), as it gives users a complete overview of the IMPILO ecosystem. Following the logic of most social networking platforms, IMPILO users can view, like and comment on the posts of their friends and members of their Circle of Trust and Care Team. They can also make their own posts that may contain text, images, links to articles, health reviews from doctors etc. A contextual menu is available in order to share a post to any other application.

Figure 3. The Timeline Tab of IMPILO app

Figure 4. The Messaging Tab of IMPILO app

Users can communicate with each other not only through their posts but also by using the messaging component of the application (Figure 4). There, they have access to their list of chat conversations and can start a new one with someone that belongs to their user groups. Apart from text messaging, file sharing is also enabled.

Users can be informed about most of the actions taken place in the application by the Notifications tab. The shortcut for this feature is almost always visible and thus accessible to the users from all the other interfaces. Notifications generally cover all events in the application from posting to the timeline to managing friend requests. In addition, through notifications, it is possible to perform various functions, such as accepting requests for the convenience of more advanced users. Finally, users can see the status of the outgoing requests they have made, through the corresponding tab on this interface.

3.2. Medical Services

There are many functionalities and features included in the application that aim to facilitate the counselling as well as the remote provision of medical services to patients by the doctors belonging to their Care Team.

By navigating to the “Health Review” interface and following some simple steps, users can seek direct advice from a doctor. Specifically, they select a doctor from whom they want the review, and then add additional information they believe is important and describe the problem that they are worried about (Figure 5). From the doctors' point of view, they can accept or reject the pending requests, and then they can complete them and respond to the patients at any time.

Figure 5. New request for Health Review

As a supplement to health reviews, the “Health Score” component is an innovative system that enables users and members of the Circle of Trust and Care Team to monitor their health over time. It is based on the EQ-5D questionnaire [14], which contains general health questions. It is specially designed to be completed easily and quickly by all users of the application, even by the least technologically trained, and the results as well as the calculated scores are easily accessible by both patients and doctors. The data of all the past questionnaires are also presented through a ‘History’ tab.

On the other hand, through the “Appointments” tab, users can have an overview of the medical appointments they can book and manage through the app (Figure 6). Specifically, after choosing the doctor and the type of appointment they wish to book, they navigate to a new interface where they enter a range of dates and thus are presented with a list of available hours for the appointment. After selecting the time and date, their request has been submitted and must be confirmed by the doctor. In addition to the appointment booking function, users have an overview of their already scheduled and pending appointments.

The types of appointments that are supported through the app are: visit to doctor’s office or clinic and tele-appointment. The latter is done easily through a module integrated in the platform. When the scheduled time of the tele-appointment comes, both patients and doctors follow the links where they connect automatically online, without the need for additional information. Users can pay for their tele-appointments in a secure and transparent manner using Stripe, a payment gateway used

to make payments on the web [15]. The payment process is done through the use of credit and debit cards (Figure 7).

Patient	Date	Time	Verification
Ioannis Kouris	2021-01-14	09.30	Teleappointment

Figure 6. The Appointments Tab of IMPILO app

Figure 7. The payment process through the app

3.3. Communication with Third Party Systems

The IMPILO app uses REST APIs to provide users with access to data that are included in their Individual Electronic Health Record, implemented by the e-Government Centre for Social Security [16]. After providing the necessary credentials and permission to access their data, patients can overview a range of information, such as their personal and family history as well as data related to vaccinations, visits, examinations, diagnoses, medication, and appointments (Figure 8). Similarly, the doctors that use the app have the ability to browse the medical data of a patient, as long as they are included in their care team.

Figure 8. Users can access their medical data provided by third party systems

3.4. Blockchain Implementation

Blockchain is one of the central and most important components of the IMPILO system, as it is responsible for confirming user data and their actions within the platform. The purpose of the blockchain is therefore to act as a basis for recording all meaningful events in the application and to provide security to users for the integrity of their data.

The review and monitoring of these events is done by users through a properly configured interface. All events are divided into separate categories for both user convenience and better application performance. When

the user selects a specific event, a hash is recreated by the backend and is compared with the hash that is stored in the blockchain (Figure 9). The user is then informed about the result and thus can validate the specific action taken place.

Figure 9. Users can have access to all actions logged in blockchain history

4. Architecture

The IMPILO application is composed by five distinct parts. Firstly, the Django backend of the application which communicates with the database and all third-party systems. The flutter mobile (iOS, Android) application and flutter web server which form the front end of the application. The webrtc and coturn servers which are responsible for providing the peer-to-peer video call capabilities for the tele-appointment and lastly the Iroha blockchain nodes (Figure 10).

Figure 10. The system architecture of IMPILO

4.1. Blockchain

Similarly to other projects that are focused on the personal health management, the IMPILO project mainly utilizes the capabilities of the blockchain that relate to the immutability of stored data. IMPILO uses the blockchain ledger to log almost any action that is taken by any user in the application. Similarly to previously mentioned applications like Medrec, this is done both to ensure the integrity of the medical data and also give more control to the end user. However, compared to such projects, IMPILO takes into consideration that most people have limited knowledge of blockchain technology, especially its inner workings, making its adoption intimidating.

Blockchain Implementation Selection

The blockchain implementation used in the project must be able to support all the key features of the application. To do that, an implementation would need the following characteristics to be considered.

Private blockchain configuration. IMPILO blockchain stores only information from the application and as such its control and ownership need also to be the same as the application itself. As such, the selected blockchain needs to support a private configuration where the owner has control over who has access to it and can control the nodes that participate in it. To this effect, the blockchain used in the current project is a private blockchain [17], where only the organisation hosting the application has permission to read and write in it freely.

Non proof of work consensus algorithm. Consensus algorithms are necessary for keeping and ensuring the same data are always present in all the nodes of the blockchain, both to protect from malicious attacks and to solve basic communication issues that arise. The most common ones popularised by its use in Bitcoin was the

proof of work algorithm which uses computational power to solve difficult mathematical issues. While common, these proof of work algorithms are plagued by many issues such as, needing significant resources and being linked with environmental damage. In addition, these types of algorithms are most useful in public blockchains where some kind of reward is given to the winner node. In our private configuration this is not the case. Therefore, we need a different type of consensus algorithm.

Existence of mobile client libraries. IMPILO is designed first and foremost as a mobile application. While it has a corresponding web implementation, it is secondary, therefore to allow direct communication between the end user and the blockchain the existence of client libraries for the most common mobile OSes (iOS, Android) were necessary.

Allow creation of different roles with different permissions. In order to streamline the process for users, some of the functions need only to be completed by the admin accounts and are not needed for the users.

Allow storing of custom data. IMPILO stores hashes are produced from events in the system. These hashes need to be stored in the blockchain and either through a custom id system or through the blockchain itself. In addition, the data needed to be accessible by the admin accounts to fulfil the transactions.

At the beginning of the project, there were a number of different frameworks that supported building your own blockchain, but the only one that fulfilled all those characteristics was the Hyperledger Iroha. Iroha is a general purpose permissioned blockchain system that can be used to manage digital assets, identity and serialized data. It has dedicated libraries for the android and the iOS operating systems that allows direct access from the mobile devices. In addition, it uses “YAC” (Yet Another Consensus) algorithm [18], which allows the creation of

multiple roles, that gives permissions to accounts.

Blockchain Accounts

There are two types of accounts in the IMPILO ecosystem that each user has. The normal account that gives access to the IMPILO application itself, and the blockchain account, used in the creation and retrieval of logging information.

User accounts in the blockchain are created in conjunction with the normal application account automatically by the backend service of the application. In order to do that, the user is not in control of this process and therefore he is not the one in control of the blockchain account credentials. These are stored in the backend of the application and provided to the user client whenever direct access is needed. This is done in order not to burden the user with handling his blockchain account and contents in addition to the application account. Whether this change is positive or negative, depends on many factors and is not a straightforward answer. A middle ground could be found in using account recovery techniques such as other blockchain based applications but that comes with its own set of caveats and potential issues.

There is one additional type of blockchain account, the admin account, used by the application to handle all the functions of the backend with additional permissions.

Information Stored in Blockchain

Iroha offers two main ways of storing data. The first and most straightforward way allows storing data in each account itself in a field called account details, which stores a key value pair with the constraint that values are smaller than 4096 characters long.

The second way involves the transaction system built in Iroha itself. Iroha allows the creation and transfer of “assets” between the accounts. These “assets” are used to represent any type of commodity. In our implementation, each different asset represents a different action

completed by a user that we want to save.

For example, there are different assets for creating timeline posts, editing posts, deleting posts and commenting posts. Not every single action is saved in the blockchain because not every action taken in the app is meaningful, such as post likes. In general, only information that changes the state of the application or performed through the Circle of Trust and the Care Team features or is related to medical data, has a distinct asset and is therefore saved.

Each successful transfer of an asset also allows the transfer of 32 characters. These 32 characters are used to store a 32bit hash that contains all the details of the entry. The hash is created using the Blake2b hashing algorithm. The information saved for each entry is different, depending on the type of asset and usually contains some or most of the table fields related to each action, in a comma separated string. Since this information is hashed, there is essentially no limit to constrain us. However, in order to recreate each entry, the exact data in the exact order are needed. To ensure that these hashes can be recreated when each transaction is concluded, a copy of the data is saved in the database. An advantage of using the asset transfers is that this whole process acts as a sort of a data structure, where the assets serve as a counter of the actions. Therefore, since the order of the transfers is immutable, we can use it to correlate it to each of the actions data, without the need of additional metadata fields. This means that if any data is missing from the database, it will be immediately obvious since the hashes won't match anymore.

Flow of Information

There are two use cases during which there is a necessary communication with the blockchain:

First, creating a new record due to some action (Figure 11). This process of creating a new log is always initiated by the users themselves, when they take an action.

Figure 11. The process of creating a new record due to some action

The backend is essentially acting as an intermediary and handles the requests to the blockchain itself. One disadvantage that we detected is that either an attacker or a malicious administrator, could in theory falsify the results before they reach the user. The malicious backend could save different information or not save it at all, while temporarily showing the user the correct one. This does not require him/her to gain access to the blockchain, merely the backend. To combat this eventuality, the user can simply inspect the created data from the blockchain immediately after, since the blockchain's information is immutable.

This same process can be achieved in different ways, such as the user is communicating with the blockchain itself, which avoids the aforementioned issue. While this can be done in the background without burdening the user, it will generally cause more issues, even if it leads to a more centralised implementation. We identified a major security issue. First, in case the action fails, either due to a technical fault or a malicious attack, our chosen implementation will simply reject the action without affecting the blockchain records (Figure 12).

Supposing we had used the alternative more

decentralised method, the process is vulnerable to malicious users. In this case, to be able to execute the transaction, an appropriate asset would be given to the user blockchain account so he can initiate the transfer and log the action.

Figure 12. An action is rejected without affecting the blockchain records

Figure 13. An action is rejected and the blockchain records are affected

While this ensures that the client will be given the asset only if the action is valid, this does not currently stop him from inserting false data (Figure 13). Since the blockchain action itself is valid, this data will be saved successfully regardless. There are other blockchain implementations which could potentially offer an additional check in the content of the transaction. In our use case, this additional level of decentralisation does not offer much due to the already centralised manner that the rest of the application works, thus, the first method where the backend orchestrates the transfer of information is preferred.

The second use case involves the user trying to check the validity of the actions stored in the log of the application. This process is mildly complicated since an iroha blockchain client compatible with the flutter web framework does not exist. This has led to two slightly different processes when retrieving the information.

The first and most comprehensive process involves the mobile client directly communicating with both the backend and the blockchain itself. In the initial call, the client retrieves a preview list of the actions logged in the database. Then the user selects a specific action, whose details and validity need to be checked. Because the logs are always found in the same order, it retrieves the hashes

from the blockchain itself through calls that are independent from the backend. When it has retrieved the information from the database, it recreates the hash and compares it with the one from the blockchain. If the hashes match, then the information is undoubtedly identical.

If the information has in some way been altered or is missing completely, in which case a whole different record will be in its spot, then the hashes will not match, and the user will be informed.

In case the user initiates the process from the web client, since there is no way to communicate directly with the blockchain, the process is left to the backend to orchestrate.

In this case, both the hashed data and the proper log information is passing through the backend (Figure 14), which is not ideal since it opens up an additional vector of attack. Potential malicious users, or even if the owner of the application is acting maliciously, could in theory provide false data by hashing the same false data he provides, in which case the attacker does not even need access to the blockchain itself. This attack is not possible, or at least it is much harder to complete with the previous methodology.

Figure 14. Validation of logs is passing through the backend

Blockchain Nodes

One advantage of the blockchain technology is the high redundancy offered by the presence of multiple nodes containing the same data. In our implementation, the starting state of the system involves the blockchain being only in control of a single organisation handling the application. Iroha allows adding new nodes in the system that are hosted by different applications without necessarily giving the full access. New roles can be created that allow overview of information without allowing creation of new entries.

5. Pilots and Evaluation

In order to ensure that the IMPILO application matches the technical requirements as guided by its design and development and is defect free, a series of checks presented below were performed to ensure proper operation and acceptance by users in real time. This process is considered crucial as it involves the evaluation of the features of the IMPILO system for any missing requirements, bugs or errors, security, reliability, performance and customer satisfaction.

5.1. Technical Evaluation

The technical evaluation of the IMPILO platform was

performed by applying a series of well-known testing methods including smoke testing, compatibility testing, capacity testing, security testing and boundary testing.

Smoke testing is described as a set of tests that confirm that the system is stable and that all important functions are present and operate under normal conditions. At the IMPILO system all smoke tests were executed manually and performed prior to the decision of whether further tests should be performed. As such, the purpose of smoke tests is not to investigate for errors but to ensure stability. These manual tests were performed using Postman [19], a popular API client that facilitates the creation, sharing and testing of the APIs of interest. Through this process, all APIs were tested and responded as expected.

Compatibility testing is a category of software testing to check if a software can run properly on different browsers, mobile devices and networks. The IMPILO application was tested in various browsers, including Firefox, Chrome, Microsoft Edge and Safari. Concurrently, the application's functionality was tested in different versions of the aforementioned browsers to ensure that the application behaves the same in each version. Additionally, as the application is compatible with Android and iOS devices, both operating systems were tested for proper operation. Finally, the application was tested on different networks (3G, 4G and WIFI).

Capacity testing is a type of software control that is performed in order to determine the behaviour of a system

in both normal and peak conditions. As such, the JMeter [20] open-source software was used, an application designed to analyse and measure the performance and operational behaviour of a web application in peak conditions. The exploitation of application's behaviour was performed under a different number of users while using the application simultaneously. Specifically, when 100 users simultaneously sent a request to the application to get the measurement types (weight, height), the average response was 1.65 seconds while when the users were raised to 500, the average response increased to 11.3 seconds (Table 1). Additionally, when the number of simultaneous users was 1000, 0.5% of them failed to connect to the server while when the number of users increased to 2000 this percentage reached 36%. Results considered satisfactory taking into account the fact that the platform at this stage is connected to one server (Ubuntu 18.04, 2 virtual CPUs, 4 Gb RAM) while no load balancing has been performed as would normally happen with the inclusion of more servers in the system.

Security testing is a type of software control that reveals vulnerabilities and risks in a software application preventing malicious attacks by intruders. The IMPILO application was tested for system vulnerabilities using the Golismero framework [21]. It is an open-source framework which is used to map web applications and find vulnerabilities by integrating a number of other security tools such as OpenVas [22], DNS recon [23] and Nikto [24]. Results extracted through this process did not uncover any vulnerabilities, threats or risks in the IMPILO application which validates that the software is working towards the requirements that have been specified. These requirements include various safety protocols that have been set in the IMPILO application to ensure that there will be no breach. Specifically, when a user registers in the system must enter at least 6 characters of which there must be at least one number and one character. Concurrently, the password entered by the user during registration is encrypted when stored on the server using the PBKDF2 algorithm with SHA256 hash (Django framework, Python). This encryption is considered secure, requiring huge computational time to be breached. At the same time, a token-based authentication is performed which allows users to confirm their identity by receiving a unique token when connecting to the application. This protocol offers a second level of security so that there is detailed control over every action and transaction.

Lastly, boundary testing was performed through all APIs of the IMPILO system by entering in the various fields minimum, maximum as well as values outside the expected input limits. When maximum and minimum values were entered, the endpoints responded as expected while when values outside the limits were entered then the request did not continue and a message was presented to the user notifying that the specific request could not proceed further as the field has more characters than the

allowed limit.

5.2. Usability Evaluation

Usability evaluation aims to determine how well potential users of a system can learn and use it, as well as how satisfied they are with the process. There are a variety of methods used to evaluate the usability of a system, at different stages of the design and development process. Some of these methods are based on data from real users, while others are based solely on application usability testing experts.

For the IMPILO platform, a study to evaluate the overall design was conducted by collecting quantitative data through questionnaires. Some of the most widely used and trusted questionnaires for usability assessment are the System Usability Scale (SUS) [25], the Website Analysis and Measurement Inventory (WAMMI) questionnaire [26] and the User Interaction Satisfaction Questionnaire (QUIS) [27]. The SUS questionnaire was chosen for the IMPILO application as it can be used in a variety of products and services including mobile and software applications as well as it is cost effective and easy to complete by study participants.

Fifty two people (mean age = 38.9 years, SD = 4.5, range = 30 –50, 30 women) participated in the study evaluation of IMPILO's platform design. Participants were instructed to go through all functionalities of the platform and report their experience by completing the SUS questionnaire (1-2 minutes long). Results extracted through this questionnaire showed that participants' experience through the IMPILO platform was excellent (average SUS score 86.49 out of 100).

Additionally, participants were instructed to respond to a questionnaire specifically related to their experience on IMPILO's platform components such as patient's registration (score 4.8 out of 5), doctor's calendar (score 4.8 out of 5), timeline (score 4.8 out of 5), payments (score 4.6 out of 5), friend request (score 4.9 out of 5), interconnection with IDIKA services (AIFY, eRDV) (score 4.7 out of 5) etc. Results showed an overall satisfaction for the functionalities that the platform provides (total average score 4.8 out of 5).

6. Discussion & Next Steps

This document describes the IMPILO platform, an innovative health social networking application, in which users can store their medical records and access them from any computer or mobile device as well as share them with their doctors or relatives. From doctors' side, they can keep in touch with their patients and access their complete medical history in order to extract better personalized diagnoses. Concurrently, users and doctors are able to communicate remotely via chat messages or

schedule tele-appointments and other counselling services. The application incorporates many features that characterize social networking platforms and are aimed at communication and interaction between users.

Overall, it can be concluded that the application of Blockchain technology in areas beyond cryptocurrencies is of particular value. This is evident from the increasing research interest around Blockchain, in areas where it has traditionally not been implemented. Especially in the field of health, to which the IMPILO platform refers, blockchain can create more reliable and durable networks, while helping seamless communication between the various stakeholders (doctors, patients, hospitals, etc.). Decentralized data storage and full control of a patient's consent management process can lead to the development of solutions with increased interoperability between heterogeneous systems and more reliable provision of medical services.

A future addition could be allowing advanced users to handle their blockchain account themselves. The existing

process can be altered as mentioned before, so users are the only ones with access to the blockchain account credentials. This may prove problematic since losing the credentials would essentially cripple their account but on the other hand will offer increased security of their account, since only they will have access to it, at least as long as they follow all the proper guidelines.

Another addition could be the integration of an individual's medical data from other applications that are connected with smart devices such as glucose recording applications, heart rate recording applications, oximeter recording applications, training and activity recording applications, etc. By incorporating all this information into a health social networking platform as IMPILO, not only would help doctors extract more accurate conclusions regarding their patients' health but it could also provide valuable information in the scientific community through the collection of primary data that could lead to the development of automated or semi-automated interventions at the individual level.

Table 1. System response when a different number of users simultaneously sent a request

HTTP Request	# Samples	Average (ms)	Min (ms)	Max (ms)	Std. Dev.	Failure %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
Measurement type info	10000	39056	0	131273	54774.53	81.7%	73.05	133.20	2.35	1867.30
Measurement type info	7000	55572	0	131266	58740.8	77.1%	51.36	94.04	2.07	1874.80
Measurement type info	5000	78051	0	131270	56612.05	70.3%	36.98	67.81	1.93	1877.30
Measurement type info	3000	85006	81	131353	50131.7	53.7%	22.26	35.01	1.81	1610.30
Measurement type info	2000	67393	95	131300	49124.67	36.2%	15.00	17.49	1.68	1193.60
Measurement type info	1000	23816	227	65415	11242.28	0.5%	15.02	5.02	2.63	342.50
Measurement type info	500	11264	260	19636	5588.13	0.0%	24.75	8.03	4.35	332.00
Measurement type info	100	1650	214	3697	1128.54	0.0%	22.52	7.30	3.96	332.00

REFERENCES

- [1] "Trust, confidence and Verifiable Data Audit | DeepMind." <https://deepmind.com/blog/article/trust-confidence-verifiable-data-audit> (accessed Jul. 22, 2021).
- [2] D. N. Fphag *et al.*, "CUREX- WP2- Requirements, System Design & Use Cases," 2019.
- [3] "Iryo Network technical whitepaper: Global participatory healthcare ecosystem." Accessed: Jul. 22, 2021. [Online]. Available: https://iryo.network/iryo_whitepaper.pdf.
- [4] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, Sep. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.
- [5] "MyHealthMyData - Deliverable 11.2 Project Presentation."
- [6] "Feature Cloud - Publishable Summary of the 1st Research Period: 1st January 2019 – 30th April 2020," *Nature*, vol. 388, 2020, [Online]. Available: https://featurecloud.eu/wp-content/uploads/2020/09/FeatureCloud_Publishable-summary_20202.pdf.
- [7] P. M. Fpg, M. Fpg, P. G. Fpg, and S. M. Fpg, "Panacea - D1.1 Models of health services and of medical device lifecycle for cybersecurity," no. 826293, 2020.
- [8] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018, doi: 10.1109/MCC.2018.011791712.
- [9] G. Falco, C. Li, P. Fedorov, C. Caldera, R. Arora, and K. Jackson, "NeuroMesh: IoT security enabled by a blockchain powered botnet vaccine," in *ACM International Conference Proceeding Series*, 2019, vol. Part F148162, pp. 1–6, doi: 10.1145/3312614.3312615.
- [10] "KTDI." <https://ktdi.org/> (accessed Aug. 02, 2021).
- [11] "MediLedger - Blockchain solutions for Pharma companies." <https://www.mediledger.com/> (accessed Aug. 02, 2021).
- [12] B. Copigneaux *et al.*, "Blockchain for supply chains and international trade Report on key features, impacts and policy options," 2020, doi: 10.2861/957600.
- [13] K. Ranjan, "Bowhead Health: The future of digital health," *Electron. Des.*, vol. 65, no. 2, pp. 30–31, 2017, doi: 10.1159/000511705.
- [14] G. Balestroni and G. Bertolotti, "EuroQol-5D (EQ-5D): an instrument for measuring quality of life," *Monaldi Arch. Chest Dis.*, vol. 78, no. 3, 2012.
- [15] "Stripe Payments: Complete Online Payment Platform Toolkit." <https://stripe.com/en-gr/payments> (accessed Jul. 23, 2021).
- [16] "e-Government Center for Social Security (IDIKA)." <http://www.idika.gr/> (accessed Jul. 23, 2021).
- [17] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126, Academic Press, pp. 45–58, Jan. 15, 2019, doi: 10.1016/j.jnca.2018.10.020.
- [18] F. Muratov, A. Lebedev, N. Iushkevich, B. Nasrulin, and M. Takemiya, "YAC: BFT Consensus Algorithm for Blockchain." 2018.
- [19] "Postman." <https://www.postman.com/> (accessed Jul. 23, 2021).
- [20] "Apache JMeter - Apache JMeter™." <https://jmeter.apache.org/> (accessed Jul. 26, 2021).
- [21] "GitHub - golismero/golismero: GoLismero - The Web Knife." <https://github.com/golismero/golismero> (accessed Jul. 26, 2021).
- [22] "OpenVAS - Open Vulnerability Assessment Scanner." <https://www.openvas.org/> (accessed Jul. 26, 2021).
- [23] "GitHub - darkoperator/dnsrecon: DNS Enumeration Script." <https://github.com/darkoperator/dnsrecon> (accessed Jul. 26, 2021).
- [24] "Nikto2 | CIRT.net." <https://cirt.net/Nikto2> (accessed Jul. 26, 2021).
- [25] J. Brooke, "SUS: A quick and dirty usability scale," *Usability Eval. Ind.*, vol. 189, Jul. 1995.
- [26] "WAMMI." www.wammi.com (accessed Jul. 23, 2021).
- [27] P. Harper and K. Norman, "Improving user satisfaction: The questionnaire for user interaction satisfaction version 5.5," Jul. 1993.